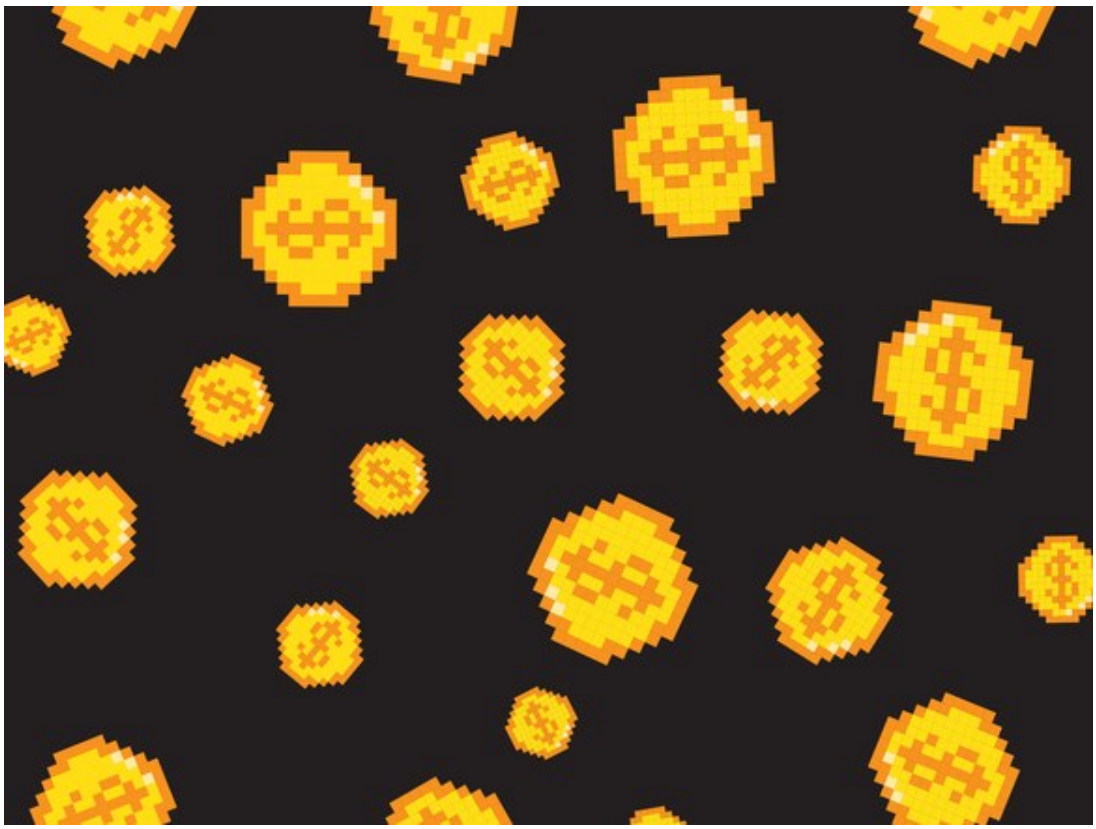
LILY HAY NEWMAN SECURITY 10.20.17 07:00 AM

YOUR BROWSER COULD BE MINING CRYPTOCURRENCY FOR A STRANGER



GETTY IMAGES

THERE'S SOMETHING NEW to add to your fun mental list of invisible internet dangers. Joining classic favorites like adware and spyware comes a new, tricky threat called "cryptojacking," which secretly uses your laptop or mobile device to mine cryptocurrency when you visit an infected site.

Malicious miners aren't new in themselves, but cryptojacking has exploded in

working instantly when you load a compromised web page. There's no immediate way to tell that the page has a hidden mining component, and you may not even notice any impact on performance, but someone has hijacked your devices—and electric bill—for digital profit.

The idea for cryptojacking coalesced in mid-September, when a company called Coinhive debuted a script that could start mining the cryptocurrency Monero when a webpage loaded. The Pirate Bay torrenting site quickly incorporated it to raise funds, and within weeks Coinhive copycats started cropping up. Hackers have even found ways to inject the scripts into websites like Politifact.com and Showtime, unbeknownst to the proprietors, mining money for themselves off of another site's traffic.

So far these types of attacks have been discovered in compromised sites' source code by users—including security researcher Troy Mursch—who notice their processor load spiking dramatically after navigating to cryptojacked pages. To protect yourself from cryptojacking, you can add sites you're worried about, or ones that you know practice in-browser mining, to your browser's ad blocking tool. There's also a Chrome extension called No Coin, created by developer Rafael Keramidas, that blocks Coinhive mining and is adding protection against other miners, too.

"We've seen malicious websites use embedded scripting to deliver malware, force ads, and force browsing to specific websites," says Karl Sigler, threat intelligence research manager at SpiderLabs, which does malware research for the scanner Trustwave. "We've also seen malware that focuses on either stealing cryptocurrency wallets or mining in the background. Combine the two together and you have a match made in hell."

What complicates the cryptojacking wave, experts argue, is that with the right protections in place it could actually be a constructive tool. Coinhive has always maintained that it intends its product as a new revenue stream for websites. Some sites already use a similar approach to raise funds for charitable causes like disaster relief. And observers particularly see in-browser miners as a

technology is worth tolerating. "Do you want ads or do you want to give away a few of your CPU cycles every time you visit the site?" Pirate Bay asked its users in mid-September. Most commenters on the feedback request supported in-browser mining if it reduced ads, but one noted that if multiple sites adopt the technique, having multiple tabs open while browsing the web could eat up processing resources.

The concerns run deeper among audiences unaware that their devices are being used without their knowledge or consent. In fact, malware scanners have already begun blocking these mining programs, citing their intrusiveness and opacity. Coinhive, and the rash of alternatives that have cropped up, need to take good-faith steps, like incorporating hard-coded authentication protections and adding caps on how much user processing power they draw, before malware scanners will stop blocking them.

"Everything is kind of crazy right now because this just came out," says Adam Kujawa, the director of Malwarebytes Labs, which does research for the scanning service Malwarebytes and started blocking Coinhive and other cryptojacking scripts this week. "But I actually think the whole concept of a script-based miner is a good idea. It could be a viable replacement for something like advertising revenue. But we're blocking it now just because there's no opt-in option or opt-out. We've observed it putting a real strain on system resources. The scripts could degrade hardware."

To that end, Coinhive introduced a new version of its product this week, called AuthedMine, which would require user permission to turn their browser into a

be circumvented and we pledge that it will stay this way. The AuthedMine miner will never start without the user's consent."

This course-correction is a positive step, but numerous cryptojacking scripts—including Coinhive's original—are already out there for hackers to use, and can't be recalled now. Experts also see other potential problems with the technique, even if the mining process is totally transparent. "An opt-in option...doesn't eliminate the problems of potential instability introduced by this," Trustwave's Sigler says. "When dozens of machines get locked up at a company, or when important work is lost due to a mining glitch, this can have a serious effect on a organization's network."

RELATED STORIES

ROBERT MCMILLAN
Inside the Race to Build the World's Fastest Bitcoin Miner

ANDY GREENBERG
Monero, the Drug Dealer's Cryptocurrency of Choice, Is on Fire

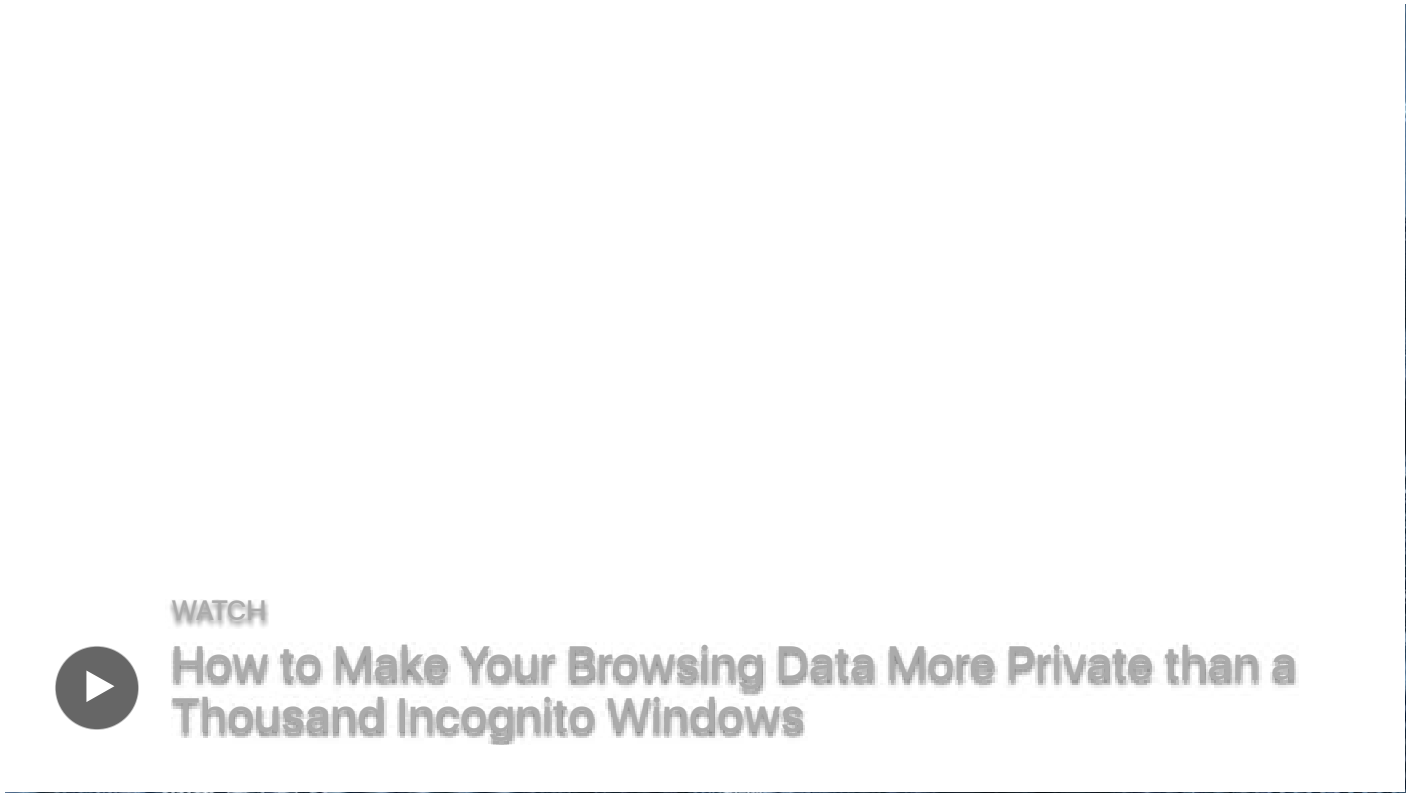
TOM SIMONITE
Bitcoin Is Splitting in Two. Now What?

And with more malware scanners on the alert, hackers will start to evolve the technology to make it subtler and more difficult to find. As with other types of malware, attackers can bounce victims around to malicious websites using redirect tactics, or incorporate Javascript obfuscation techniques to keep

complications to some. "I'm hoping that within a year we'll see even more evolution of this technology to the point where it cannot be abused by website owners who want to trick people into running these miners," Malwarebytes' Kujawa says. "But if it's only associated with malicious activities, then it might take awhile for the technology to evolve to a place that's more secure, and for anyone to trust using it."

Like so many web tools, cryptojacking has plenty of promise as an innovation—and plenty of people happy to exploit it.

RELATED VIDEO



SECURITY

How to Make Your Browsing Data More Private than a Thousand Incognito Windows

Thanks to an assist from Congress, your cable company has the legal right to sell your web-browsing data without your consent. This is how to protect your data from preying eyes.

VIEW COMMENTS

MORE SECURITY

SECURITY ROUNDUP

Equifax Found 2.4 Million More People Hit By Its Breach

LILY HAY NEWMAN

PROPAGANDA

Facebook Doesn't Know How Many Followed Russians on Instagram

ISSIE LAPOWSKY

PRIVACY

In US v. Microsoft, Decades-Old Law Leaves Few Good Options

DAVID NEWMAN

TWO-FACTOR

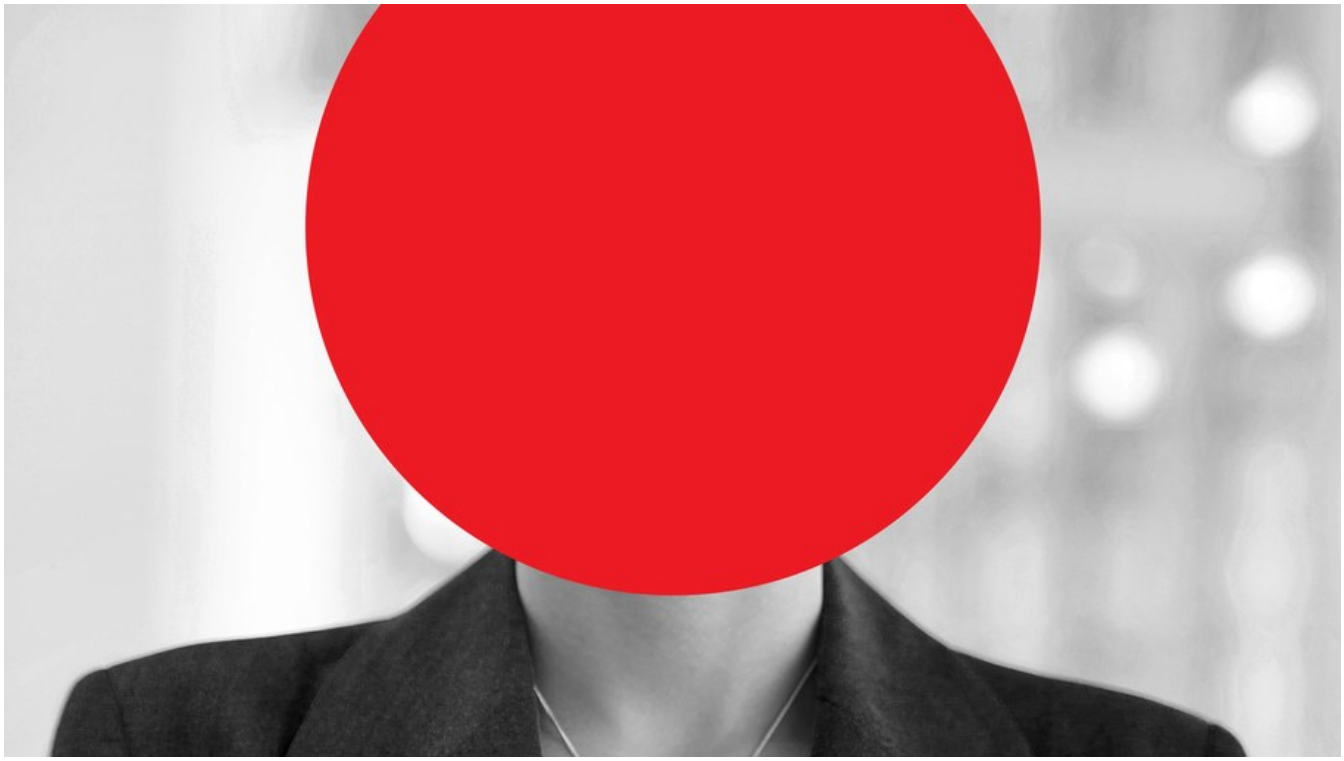
Chrome Lets Hackers Phish Even 'Unphishable' Yubikey Users

ANDY GREENBERG

INTERNET

GitHub Survived the Biggest DDoS Attack Ever Recorded

LILY HAY NEWMAN



PRIVACY

How to Turn Off Facebook's Face Recognition Features

LILY HAY NEWMAN

GET OUR NEWSLETTER

WIRED's biggest stories delivered to your inbox.

Enter your email

SUBMIT

FOLLOW US ON YOUTUBE

Don't miss out on WIRED's latest videos.

FOLLOW